



CVE-2017-12351

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-12351
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-30 09:29:00 UTC
Updated	2019-10-09 23:22:00 UTC
Description	A vulnerability in the guest shell feature of Cisco NX-OS System Software could allow an authenticated, local attacker to re

Risk And Classification

Problem Types: CWE-668

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Nx-os	7.0(3)i7(1)	All	All	All
Operating System	Cisco	Nx-os	7.0(3)i7(1)	All	All	All
Operating System	Cisco	Nx-os	8.1(0)bd(0.20)	All	All	All
Operating System	Cisco	Nx-os	8.1(0)bd(0.20)	All	All	All
Operating System	Cisco	Nx-os	7.0(3)i7(1)	All	All	All
Operating System	Cisco	Nx-os	8.1(0)bd(0.20)	All	All	All

References

Reference	Source	Link
Cisco NX-OS System Software CVE-2017-12351 Local Unauthorized Access Vulnerability	BID	www.securityfocus.com
Cisco NX-OS Flaw Lets Local Users Bypass Guest Shell Security Restrictions - SecurityTracker	SECTrack	www.securitytracker.com
Cisco NX-OS System Software Guest Shell Unauthorized Internal Interface Access Vulnerability	CONFIRM	tools.cisco.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)